Information Superiority:
Seeking Command of the Cyber-Sea

A Monograph
by
Major Thomas J. Kardos

School of Advanced Military Studies
United States Army Command and General Staff College
Fort Leavenworth, Kansas

Second Term 99-00

SCHOOL OF ADVANCED MILITARY STUDIES

MONOGRAPH APPROVAL

Major Thomas J. Kardos

Title of Monograph: ***Information Superiority: Seeking Command of the Cyber-Sea***

Approved by:

_____ **Monograph Director**
DR Robert M. Epstein

_____ **Director, School of Advanced Military Studies**
COL Robin P. Swan, MMAS

_____ **Director, Graduate Degree Program**
Philip J. Brooks, Ph.D.

Accepted the 23rd Day of May 2000

Abstract

INFORMATION SUPERIORITY: SEEKING COMMAND OF THE CYBER-SEA
by Major Thomas J. Kardos, 62 pages.

This thesis examines the initial effort to formulate principles for information-based operations. Although it is impossible to explore each aspect of this transformation, it is worthwhile to examine current efforts by the US military to develop a doctrinal foundation for Information Operations (IO). It explores the ongoing struggle to capture within the confines of Joint military doctrine those critical features of this "new age driven by information".

The world community is increasingly dependent on reliable information traffic. Information has become a commodity and source of power unto itself. Alvin Toffler describes this period as the transformation of societies from 'second-wave' (industrial/mechanical) to 'third-wave' (information-based) means. The growing dependence of the US military on these infrastructures reveals potentially vulnerable elements of the National Information Infrastructure (NII).

This monograph examines the need for a comprehensive IO doctrine. It yields a critical analysis of existing doctrine, illuminates several flaws within the current construct, and concludes with a suggested model for IO development. Doctrinal models are developed for the Army, Air Force, and Navy respectively. These models explain those aspects which most essentially describe the 'doctrinal culture' of each service component. These factors include: service organization; employment of forces (both in peace and during crisis); and methods of control. In turn, each component model is compared to the revised IO model.

Current IO doctrine provides little in the way of enduring principles and mistakenly incorporates a narrow range of offensive options. IO principles should follow the 'cultural perspective' found within present naval doctrine (a service whose doctrinal development is also at its genesis). A reformulation of the basic IO tenets is necessary to produce doctrine which is adaptive, useful, and appropriate, both in peace and in war.

TABLE OF CONTENTS

Section 1- Introduction

> *"**Information security** takes on added importance in this new age. This will be true whether we find ourselves engaged with a sophisticated foe or involved in a low-intensity conflict. On the other hand, as we look at our opportunities for offensive information operations, we will be more limited to situations when we face an opponent who has a similar reliance on information. My point is that we run a tremendous risk if we look at information warfare only as a unique American advantage."*
>
> *GEN Ronald Fogelman, Air Force Chief of Staff, 1995*[1]

GEN Fogelman's words are appropriate to introduce an understanding of the impact that information and technology are having on international life and US national defense. Granting that it is impossible to address all related consequences, it is worthwhile to examine current efforts by the US military to develop a doctrinal foundation for activities concerning information and information systems - termed, Information Operations (IO). This thesis will explore the ongoing struggle to capture within the confines of military doctrine those critical features of this "new age driven by information"[2].

One could reasonably ask how the national defense establishment became so suddenly and inclusively mired within this alteration to world politics and technical geometry. The post-Cold War world of the 1980's and 90's experienced an unprecedented evolution in global political and military power. From this, the United States has emerged as the preeminent global influence not only in military means, but in economics, technology, and education as well. Concurrently, the fracturing of this notably convenient bi-polar world ushered in an Age of Globalism. A single, compelling force can be identified at the root of this change - the rapid, unconstrained, and ever-expanding exchange of information and related technologies.

The rampant advance of technology during the latter half of the 20th century has been remarkable. This explosion in information-based systems reorders the way in which global interaction takes place.[3] The world community is increasingly dependent on reliable information traffic. It has become a commodity and source of power unto itself. Alvin Toffler describes this period as the transformation of societies from 'second-wave' (industrial/ mechanical) to 'third-wave' (information-based) media.[4] "For much of the developed world traditional measures of political and economic strength, such as territorial holdings and manufacturing infrastructure, have been supplanted by the possession and exploitation of the technical-information domains."[5]

"Technology now enables adversaries to target America's population and critical infrastructure, a capability previously only the Soviet Union possessed."[6] The advent of the internetted world of the 21st century exposes the US to groups of potential dangers, including: unauthorized users, insiders, terrorists, nonstate groups, unfriendly media, foreign intelligence services, opposing militaries, and political opponents.[7]

The growing dependence of the US military on these infrastructures bares potentially vulnerable elements of the National Information Infrastructure (NII).[8] Unfettered access to advanced technologies and limitless amounts information have effectively nullified the territorial security America once enjoyed. The deescalation of the thermo-nuclear gambit has been equalled by pervasive threats to civilian and defense systems - a peril brought about by information assailability.

The end of the Cold War and the emergence of information-technical domains mandate that the Department of Defense (DoD) expand the way in which it protects the nation and its interests. "Countries acquiring new military capabilities with interests inimical to the United States continue to exacerbate the current political arena."[9] However, as the US proceeds headlong into this quarter, others are developing related but unique strengths for which the US is less prepared.

A 1997 Rand study pointed out that while the US has thusfar retained a military-information advantage, "potential adversaries, especially nonstate adversaries, may have a lead in regard to a comprehensive information-oriented approach to social conflict. Here, the US emphasis may have to be on defensive measures".[10] So while "our current capabilities are adequate to defend against existing information operations threats, the increasing availability and decreasing costs of sophisticated technology to potential adversaries demand a robust commitment to improve our ability to operate in the face of information threats..."[11] The armed forces must develop baseline precepts to establish both offensive and defensive measures needed to retain tenor on the world stage.

This thesis will examine initial, national-level efforts to formulate principles for information-based operations. Specifically it will address the adequacy of Joint Information Doctrine. Before an assessment can be made, the purpose of doctrine must be established.

Joint Publication 1-02, DoD Dictionary of Military and Associated Terms, defines doctrine as the "fundamental principles by which military forces or

elements thereof guide their actions in support of national objectives."[12] While this definition serves as an acceptable overview, it says little of what doctrine contains. Research indicates that doctrine serves as military policy - more enduring than current political policy.[13] The Army's manual, Operations, continues that doctrine describes the principles from which to organize, train, and equip the force.[14] It provides a common '*cultural perspective*'[15] describing how to think about operations in war, peace, and operations other than war.

Section 2 summarizes those factors which mandate the formation of comprehensive IO doctrine. Section 3 explains the context of Information Operations, as well as, an articulation of current interservice designs. This sets the framework for examining existing principles and strategies. Section 4 yields a critical analysis of current doctrine, illuminates several flaws within the construct, and concludes with a suggested model for future development.

In that much of current doctrine is based upon precepts from the past, an exploration of existing doctrinal models is warranted. Sections 5, 6, and 7 examine the doctrines of the three Service Components. Models are developed for the Army, Air Force, and Navy respectively. Due to space restrictions, the models are limited to those aspects which most essentially describe the 'culture' of each service. These factors include: service organization; employment of forces (both in peace and in war); and methods of control.[16] In turn, each component model is compared to the IO model developed in Section 4.

This thesis is not meant to be overly critical of current Joint Information Operations Doctrine. It is well-understood that discerning each mien of this

diverse and enfolding discipline is a difficult task, especially for concepts very much in their infancy. However, doctrinal development must have a firm base from which to proceed.

Comparison of these several models will demonstrate that current IO development is ill-founded. It furnishes little in the way of enduring principles and mistakenly draws from a narrow range of offensive features found within Army and Air Force doctrine. This examination further relates that IO principles should emulate the 'cultural perspective' founded by the doctrine of the US Navy (a service whose doctrinal development is also at its genesis). A reformulation of the basic IO tenets is necessary to produce doctrine which is adaptive, useful, and appropriate, both in peace and in war.

Section 2 - The Call for National Information Security

"The national security posture of the United States is increasingly dependent on our information infrastructure. These infrastructures are highly interdependent and are increasingly vulnerable to tampering and exploitation. Concepts and technologies are being developed and employed to protect and defend against these vulnerabilities; we must fully implement them to ensure the future security of not only our national information infrastructures, but our nation as well."

1997 National Security Strategy[17]

"The US is the most advanced society in the world, but by the year 2020 most of the world will have been transformed by the Information Revolution."[18] As unrestricted commerce in info-technical products grows, "it is increasingly difficult to control the flow of sensitive information and regulate the spread of advanced technologies that can have military and terrorist uses".[19] While informational exploitation grants a competitive edge, so too does the rapid global transference of technology increase vulnerabilities.

It may appear that the impact of recent developments seized the nation and its military unprepared. This assessment is not an accurate. Notwithstanding its mode or purpose, the ability to receive, record, and convey information has been an intrinsic part of organized social life since the birth of civilization. However, until supported by the advances of modern science, the speed at which information was propagated relegated it to a position of secondary influence.

The technological progress of the 20th century reshaped world order in many ways. While these developments provide previously unequaled capacity to harness of information resources, the burden of their expense has been, until recently, prohibitive to all but the most financially stable nations and institutions.

During the Cold War, the US and USSR applied utmost venture to their bilateral, ideological competition. Technical developments materialized in a singular medium for preserving global position. For all these efforts, the crowning achievement became literally and figuratively expressed in the form of intercontinental nuclear capability. While related technologies allowed for discovery and invention in other areas, such as microcircuitry, communications, and space exploration, each remained subordinate to the coercive and domineering power of 'The Bomb. In the bipolar world, nuclear parity was essential for balance and effectively allowed for no other participants.

With the collapse of the Soviet Union, the world community is able to breathe a collective sigh of relief. As this transition takes place, exchange of 'spin-off' technological hardware and brainware flourishes. The intellectual products of this post-WW II duel are becoming prevalent and powerful commodities.

As information traffic becomes more commonplace, so too has the requirement to safely gather, store, manipulate, and convey information, anywhere - anytime. "These capabilities have become essential to modern economic, social, political, and defense sectors and are central to the process of using information to create competitive advantage."[20] Continual and ever-increasing worldwide interaction has produced a pseudo-community - a Global Information Environment (GIE).[21] As governments, institutions, and industry explore this new environment, innovative concepts emerge which redefine national identity. Today countries, international organizations, and even

individuals must consider themselves subelements of the GIE, much as nations once did within traditional continental confines.

With nuclear jeopardy now diminished, attention turns to the surety and vulnerability of information itself. Physical protection from hostile assault no longer provides assurance. The suffusive connectivity of new environments bears contingent risks herebefore unaddressed. As with issues of national identity, novel concepts for information stability and defense are evolving.

Throughout the past decade the US explored the implications of this new paradigm. In 1996, President Clinton identified the need "to examine vulnerabilities to the nation's core infrastructure".[22] The following year, the President's Commission on Critical Infrastructure Protection identified eight key and interdependent systems deemed essential, potentially vulnerable, and worthy of national level protection. This Minimal Essential Information Infrastructure (MEII) includes: electrical power utilities, gas and oil storage and portage consortiums, water, telecommunications, finance, transportation, emergency, and government services.[23] Once provisory systems are considered, hardly anything is excluded.

The growing "reliance on technology makes protecting US infrastructure against hostile Information Operations a paramount mission."[24] As the preeminent military establishment in the world, one might wonder if conventional superiority is sufficient to protect the MEII; this is not the case. "The demonstrated US conventional military supremacy moreover has driven our adversaries into the search for effective supra- and sub-conventional weapons

and strategies"[25]; primarily in the sphere of information weaponry. So has come the birth of the burgeoning fields of Information Operations and Information Warfare (IW).[26]

The 1997 National Defense Panel stated that: "The importance of maintaining America's lead in information systems - commercial and military - cannot be overstated. Our nation's economy will depend on a secure and assured information infrastructure. Given the importance of information - in the conduct of warfare and as a central force in every aspect of society - the competition to secure an information advantage will be a high stakes contest..."[27]

Countries previously unable to afford conventional forces and arms must now be considered. Emerging threats provide strategic intelligence challenges manifest warning and attack assessment problems. The nature of the 'information battlefield' blurs traditional boundaries of war. Unseen and non-existent peripheries raise complications in building and sustaining international coalitions. Perception management becomes an influential component. IO conflict goes beyond traditional military frameworks, to include: espionage, terrorism, economic competition, and efforts to control global public opinion.[28] The effect is an overall increased vulnerability to the US homeland.[29]

As the national civilian leadership turned attention to the implications of these emerging threats, then Chairman of the Joint Chiefs of Staff (CJCS), GEN Shalikashvili, introduced the concept of military Information Operations (IO). In 1996, he commissioned the research and publication of 'Joint Vision 2010'.[30] JV 2010 described a Military Information Environment (MIE) which, like its global

and national counterparts (supra-systems), consists of information systems and organizations - friend and foe, military and civilian, that support, enable, or significantly influence military operations.[31] The culture of warfare for the US was forever changed.

It is apparent that this technology is at the "core and foundation of this military revolution, because information and knowledge change[s] the previous practice of measuring military strength by simply counting the number of armored divisions, air force wings, and aircraft carrier battlegroups".[32] Realizing that "the speed and pervasiveness of data transmission in the Information Age are causing a revolutionary change in the nature of military operations and warfare"[33], the Joint Staff set to work to establish the proper role for the armed forces in protecting the MEII. As defense specialist, DR Robert Stark, notes: "If the US grand strategy is selective engagement, then *information superiority* is warranted in order to provide greater understanding of the strengths, weaknesses, and centers of gravity of an adversary's military, political, social, and economic infrastructure."[34]

"Recognition that the military is amidst the throes of a Revolution in Military Affairs (RMA) is not sufficient to produce necessary and meaningful change. A strategy is required to chart the course for the near future and beyond. This concept is formulated in programs and has come to be known as"[35] the Joint Doctrine for Information Operations.

Section 3 - The Genesis of IO Doctrine

> *"We must have **information superiority**: the capability to collect, process, and disseminate an uninterrupted flow of information while exploiting, or denying an adversary's ability to do the same. There should be no misunderstanding that our effort to achieve and maintain information superiority will also invite resourceful enemy attacks on our information systems. **Defensive information** warfare to protect our ability to conduct information operations will be one of the biggest challenges in the period ahead."*
>
> *Joint Vision 2010, 1996*[36]

Joint Vision 2010 furnishes the framework for future Joint Doctrine. This construct defines four fundamental principles: Dominant Maneuver; Precision Engagement; Focused Logistics; and, Full-Dimensional Superiority. Concurrently, a unifying factor is identified to integrate these principles: *Information Superiority*. In 1999, CJCS GEN Shelton stated that: "Information Operations and Information Superiority are at the core of military innovation and our vision of the future. [It] provides the conceptual template for the ongoing transformation of our military capabilities..."[37].

JV 2010 defines Information Superiority as "the capability to collect, process, and disseminate an uninterrupted flow of information, while exploiting or denying an adversary's ability to do the same."[38] Information is the essential foundation of knowledge-based warfare.[39] The evolving environment will fundamentally change the way in which the military operates in peace and in conflict.[40]

The basic principles for information operations are contained in Joint Publication 3-13, *Joint Doctrine for Information Operations* (JPub 3-13, 1998). A doctrinal model for Information Operations will highlight the principles guiding IO organization, employment, and control, therein describing the 'cultural

perspective' taken by the military within this emerging domain.

JPub 3-13 defines Information Operations as "actions taken to affect adversary information and information systems while defending one's own information and information systems. They apply across all phases of an operation, the range of military operations, and at every level of war."[41] They take place in peace and in war and are further defined as either offensive or defensive.

Offensive IO are those actions taken to exploit, corrupt, disrupt, degrade, or destroy information, information systems, and human will in support of friendly military objectives.[42] Defensive IO are conducted to protect and defend friendly information and systems, enable timely, accurate, and relevant information passage while denying the enemy the ability to exploit friendly information and systems.[43] In peace they are part and parcel to every military endeavor. In crisis and war, IO is designated Information Warfare - IW - whether offensive or defensive.[44]

The doctrinal model will be developed and examined in the following section. In doing so, it becomes evident that although JPub 3-13 is quite extensive (over 120 pages), it fails to define a viable theme - that is, the publication is a description of actions and planning axioms with limited substance to guide adaptation within the Information Environment.

Section 4 - The IO Model and Doctrinal Shortfalls

Information Superiority: "The concept is rooted in the indisputable fact that information and information technologies are increasingly important to national security in general and to warfare specifically."

Martin Libicki[45]

The purpose of Information Operations may appear self-evident from its definition: "actions taken to affect adversary information and information systems while defending one's own information and information systems."[46] Regrettably, this "definition is so broad that it includes everything, thereby making meaningful discussion of IO issues impractical, if not impossible".[47] But to regard the subject as obsolescent solely on this account would be sophistic.

To appreciate the 'culture' established by current Joint Information Operations Doctrine, one must consider to what extent the doctrine disciplines purpose through organization, employment, and control. Effective IO ensure that friendly information is timely, accurate, and manageable.[48] They protect sensitive information from access by adversaries and can be used to manipulate, degrade, and deny information available to hostile parties.[49]

Defining IO organizations presents some difficulties in that these activities are inherent to all other forms of military operation. In many ways information can be viewed as an organizational function; an element of combat power considered during planning and execution.[50] DR Robert Stark points out: "Information Superiority is only effective if the adversary has an information architecture that can be destroyed (read - 'affected')."[51] Therefore, the effort must be tailored to the environment. In essence, "the architecture of the opponent's information infrastructure determines [the] effects of IO and IW

efforts." JPub 3-13 directs commanders to establish fully functional IO 'cells'.[52] Regrading the composition of these departments, the JPub describes broad considerations that should be applied. Within these general planning guidelines, the IO effort is divided amongst the staff (J2, for intelligence and information security; J6, for Command, Control, Communications, and Computers; and, J5, for strategic plans and policy).

The greater part of JPub 3-13 is dedicated to principles of employment. It rightly points out that the effectiveness of information operations "comes when IO is planned and integrated early in the planning process."[53] In fact, they are most prolific when undertaken during times of peace. The JPub adds that: "Combatant Commanders have [the] responsibility to integrate IO into war plans and daily activities."[54] These operations are as much about maintaining peace as they are about achieving a decisive edge in war.

Information Operations occur throughout the continuum of military activities. It would be fitting to catagorize ongoing IO as either Information Warfare or Information Peacefare. While the JPub begins by stating that they occur in peace and conflict, they are classified as either offensive or defensive.[55] Chapters 2 and 3 of the joint publication are dedicated to these enterprises. Chapter 4 speaks to the roles and missions of information planning groups, as Chapter 5 defines planning methodologies.

The doctrine extensively profiles instruments for conducting offensive and defensive operations. These agents include: operations security (OPSEC), psychological operations (Psyops), electronic warfare (EW), military deception,

physical destruction, civil affairs (CA), and public affairs (PA).[56] It introduces concepts, such as computer network attack and defense (CNA/CND); information assurance; counter-propaganda; and personnel security.[57] As with the Global Information Environment, it would be difficult to find an area that could not be included under the guise of this IO framework.

In forming an IO model: Their purpose is to maximize the benefits achieved by continuous information control, while refusing the enemy the same - in times of peace, transition, and crisis. IO are integrated into plans and operations at all levels, which aim to achieve and maintain Information Superiority through *information control.* This definition is too imprecise, however, to allow one to visualize IO in total.

It is appropriate at this point to question why the current manual produces such ill-defined, unbalanced concepts. The propensity of IO objectives toward the offensive is understandable from two perspectives. First, it is generally accepted that the military is organized, trained, and equipped to *fight* and win the nation's *wars*. Secondly, the very definition of IO, *"actions taken to affect adversary..."*, implies that an opposing force exists which can be clearly identified and against which IO efforts can be directed. In doing so, the doctrine better describes an environment in which such functions occur, rather than a more clearly defined organization.

The context of IO is so broad that the doctrine is notably nonspecific in most areas. A coherent plan for organizational integration is lacking. The

doctrine is abjectly one-sided. Passing mention is made of peacetime engagement, with a greater part of doctrinal text centering on techniques and procedures for crisis employment. While it might serve a useful guide in time of war, it assumes a clearly defined set of goals and objectives which are unlikely to exist during peace and operations other than war.

In order to properly consider Information Operations or Information Warfare, a concept for the operational environment must be defined. IO is in a sense an environment unto itself. While this poses a dilemma, the JP circumvents this difficult area by restricting its definition to information infrastructures, the media through which offensive and defensive operations take place.[58] This limited abstraction reduces IO and IW to tangible means and definitive methods - a shortfall which soon becomes apparent.

It should be acknowledged that "the Joint Staff has faced great difficulty in assigning precise responsibilities even for military forms of information [operations and] warfare"[59], much less contingent activities involving non-military, domestic, civil, commercial, and foreign entities. It is unclear which aspects of IO are subordinate to others, as well as, the authority of military commanders over non-military institutions and actors.[60]

The information environment has no fixed boundary.[61] As such, the environment is as nearly a condition as it is an arrangement of things. Because information operations extend within and beyond all national dealings, they must be integrated and support one another. In this context, Information Superiority escapes definition. To be informationally superior in the absolute sense, one

must achieve superiority in every tangential system as well - an impossible task indeed.

Confronting peacetime operations, the manual accepts that theater commanders are best able to determine requirements. These commanders must consider foreign, domestic, and customary laws, treaties, agreements, as well as, the structure and relationships among government and non-government entities.[62] Nonetheless, a definitive explanation of duties, responsibilities, and authority is not addressed in detail. Local commanders must determine what peacetime actions are appropriate.

Due to the all-encompassing environment which makes up the IO environment, combined with the "truly sophisticated [means of conducting IO] warfighting, it is difficult to ascertain where planning ends (peacetime operations) and execution (war) begins".[63] Peacetime information engagements are difficult to specify and design, and accordingly the manual only addresses the topic of war in detail. JPub 3-13 addresses information warfare as early as the second page of the manual. Unfortunately, this produces a 'combatant' doctrinal culture.

This indistinctness between peacetime engagement and wartime action arises within the basic definition of Information Operations. The doctrine dedicates considerable space for applying the Principles of War to information operations[64], with the remainder focused on Offensive and Defensive planning and execution. Fundamentally, IO is used as a means to reclassify already inherent capabilities under new and inadequately defined concepts.

Current IO doctrine has "no apparent focus as efforts appear specialized

and non-complementary".[65] The operational formula is incomplete. As Vincent Bryant states; IO doctrine has "too much offense, too much technology, too much optimism, too much intellect, and too much warfare".[66] Underlying precepts are needed, not specific procedures. What might such a doctrine look like?

A more reliable interpretation would offer information and information systems as the ends, ways, and means necessary to advise decision-makers and cast operation environments in both peace and war. It would not be merely the sum of current military capabilities under a different title. Continuous forms of information engagement would seek to achieve information control. For this, long standing policies, treaties, agreements, and etiquettes would be established, understood, and enforced within all sectors of the information environment.

The functions of information operations would produce forces organizationally tailored by local commanders to achieve higher objectives. IO would be integrated into all operations as a proactive means to shape and maintain peace, yet achieve conditions desired during conflict. IO would be executed as much from the structure of the organization as from the unifying role it serves in defining the environment. Information engagement would not be just about winning wars, but about very existence in the Information Age - protracted issues requiring long term, gradual solutions.

A final, revised IO model can be summarized with the purpose to gain and maintain *information control*. IO forces exist and methods are employed *in*

peace to shape - in crisis to gain control. Employment is governed by a clear sense of which actions, postures, and methods are considered *friendly*, *hostile*, or *neutral*. Finally, the model requires that the IO engagement be continual, adaptive, created at the highest national levels, yet responsive to the supported commander.

While Information Operations appear the product of revolutionary technologies and theories, it does not follow that all ideas of the past and present are inapplicable. Doctrinal concepts can come from many sources: current policy, available resources, strategy and campaigns, past doctrine, threats, history and lessons learned, strategic culture, fielded or emerging technology, geography, demographics, and types of governments.[67] Of the many, a major influence is existing doctrine.[68] In the next three sections the fundamental principles defining current service component doctrine are examined. In turn, doctrinal models for the Army, Air Force, and Navy are compared to the revised IO model developed above.

Section 5- Army Doctrine and "Land Dominance"

"As the armed forces restructure and decrease, their missions are changing from those of the Cold War's forward-deployed force to more complex missions of a post-Cold War ***expeditionary force.***"

DR Jacob Kipp[69]

With the collapse of the former Soviet Union, the concurrent increase in small scale contingencies, and the effects of modern technologies, the Army has set about to redesign the way in which it structures and employs its forces. It has been proactive in updating many of its principle publications to address post-Cold War innovations.[70] The keystone doctrinal manual, FM 100-5 - Operations, captures the Army's approach to organization, training, material, and leader development.[71] However, the current version (June 1993) is considerably out of date in light of ongoing initiatives within the Joint community. The Army continues to wrestle with numerous technical and operational issues, effectively delaying publication of an updated and complete doctrine. Despite this, the service is not without published guidance to direct interim modernization efforts.

The vision of the future force in light of forecasted requirements is defined in the Army's TRADOC Pamphlet 525-5, Force XXI.[72] The pamphlet calls for a top-down reconsideration of the Army's current role and employment criteria, thereby prompting a comprehensive reorganization initiative. Although not authoritative, Force XXI describes six (6) Patterns of Operations which replace Airland Battle doctrine of the 1980s and 90s. The operational patterns include: Project the Force; Protect the Force; Gain Information Dominance; Shape the Battlespace; Decisive Operations; and, Transition to Future Operations.[73] While it must be recognized that this doctrine is transitional, a preliminary doctrinal

model can be developed from the above 'patterns'.

The most apparent organizational change within the Army has been the wholesale decrease to the size of the force. It is no longer politically nor economically viable for the US to maintain a large standing army. During the past ten years the active component has been reduced from nearly three quarters of a million soldiers to a force stabilized at 485,000.[74] This drawdown has been accompanied by the withdrawal of forces from foreign posts and similar reductions to defense arrangements over seas. The cumulative effect is a turning away from the Soviet-focused tenets of the mid-1980s, with its massive active-duty force and extensive global infrastructure.

Force XXI acknowledges that future military organizations will be fewer in number and more modular and tailorable in design.[75] These CONUS-based (continental US) units will be organized around common, generic tables of organization and employed in any conceivable size and configuration. Similarly, declining overseas structures mandate that logistical support agencies maintain the capability to supply a myriad of potential force arrangements.

An increasing dependence upon the nation's Reserve and National Guard forces has developed. Operations of considerable size or duration now require the mobilization of the nation's inactive force. Additionally, the US is becoming reliant on the cooperation of coalition forces to accomplish even the most rudimentary missions in foreign lands.

The wholesale reduction to active force numbers, combined with the changing dynamics of the global political and technological environments have

profoundly affected the manner in which commanders train and employ forces. With decreased forward presence comes the coincidental requirement that forces be "rapidly deployable".[76] "The forward deployed forces of the past are being replaced by forces prepared for world-wide short notice contingency operations across the spectrum of conflict."[77]

The drawdown has generated notable changes in US daily interaction with foreign armies. This is reflected in the most recent National Security Strategy (NSS-1999), which states:"... sustaining our engagement abroad over the long term will require the support of the American people... and, when necessary, with military force".[78] The relegation of military engagement policy is further reinforced by a perceived reluctance to use such exercises as a regular form of Army employment. The NSS continues this theme as: "Such uses of military forces should be selective and limited..."[79]

The decline in habitual and continuing contact with other armies and environments and the requirement for worldwide deployability have altered the way in which the Army prepares for war. The smaller force must now concentrate on an ever-increasing range of employment possibilities and locations. Regional specialization has become a luxury of the Cold War past, as the focus turns to broad capabilities and effects. To maintain readiness, the Army must make liberal assumptions about future political and military environments.

Future employments will be characterized by economies of force and scale. Commanders will deploy with smaller, modular, tailored, mission-oriented

units - leaving unneeded forces at home stations prepared to respond to separate contingencies. Units will draw support wherever available, from both near and distant locations. They will activate only after threats are identified and goals established. The size and capability of the standing force mandates quick, decisive outcomes. If this is not feasible, a recall of reserve forces will be necessary, as well as, reliance on allied support.

Doubtlessly, the changing environment will have profound effects on control mechanisms. Control of wartime forces must be enhanced by early establishment of purposeful goals. In peace, continental forces will rely heavily on the clarity of their doctrine. More than other service components, Army doctrine tends further toward defined procedures for specific tasks.[80] Peacetime doctrine is essential in formulating practical tactics, techniques, and procedures upon which to develop training and forcast employment scenarios.

As technology alters the ways in which forces move, communicate, and fight, the Army's view toward its end purpose has not changed significantly. Its role remains to achieve "*dominance on land*, where the decisive element of victory for our nation has always been critical".[81] Despite advances in speed, method, or control, attention to the physical realm is unchanged - gain 'Land Dominance'.

The model of the Force XXI Army is summarized by a small, offensively-oriented, continentally-based force trained to engage a wide variety of threats across the full spectrum of war. It is characterized by the tenets of modularity, scalability, and tailorability.[82] "In force projection operations, commanders [will]

depend on small, deployable teams"[83], capable of swift action during "regional conflicts; crisis response; power projection; joint, coalition, and interagency operations".[84] It will depend upon rapid, decisive operations with clearly established goals, ultimately relying on the ability to inflict physical destruction upon an enemy. Physical control is its primary mission. The Army has staked its future on these premises - but are these concepts from which an IO doctrine can be derived?

The reality envisioned by the future Army model does not transfer favorably to Information Operations. Methods for information engagement and warfare cannot be developed in the vacuum of a continentally-based force. Information organizations must exist within, adapt to, and be adapted by the everyday global environment. Information employment by selective force projection effectively removes these activities from the ever-growing, complex world.

Small tailorable IO organizations of limited infrastructure may appear desirable when considering politics and economy of force. However, in light of the developing reach of information and related technologies, this method of organization is antithetical to IO theory. Effective structures must mirror the form of the environments and threats. At present, smaller, less pervasive designs are abjectly inappropriate.

Generic organizations presume long-standing, stable conditions from which one can respond in time of crisis. The information domains are so varied and rapidly evolving, that the notion of genericism cannot be applied.

Furthermore, adversaries might easily determine the capabilities of such predictable designs and develop effective countermeasures.

The Army owns and controls the structure and equipment it employs. The ability to adapt forces and impress physical control are exercised through the use of specific orders, operations, and exercises. The information environment is global and indistinct. Information organizations do not provide for clear definitions of structure. In this info-arena, orders and instructions will inevitably involve a host of ancillary, unforeseen elements and effects.

Generic IO forces would lack the specialization needed to maximize information effects. A withdrawal from daily engagement and employment would leave military information operators isolated from evolving technologies and potential threats. Habitual isolation, when combined with the premise of rapid, limited response, limits the range of options available to planners. Information awareness and skill can only be achieved with ongoing contact with global events.

Reliance on information reserves and coalitions introduces new paths of vulnerability. IO reserves will fall victim to frailties akin to those of disengaged active forces. The capability of these reserves to respond to unfamiliar information environments would be minimal. Likewise, the benefits which coalition forces bring to physical conflict are equaled by a host of security risks.

The concept of force projection might appear appropriate to an environment where information passes at the speed of light. Again, this runs counter to the precept that IO must be ongoing - shaping the information world

as it progresses and develops. To apply rapid projection and selective engagement principles would be to produce an IO force that is *reactive,* not *adaptive*. Operating in this way is to begin from a position of weakness, with actions driven by an adversary, rather than shaping and quelling hazards as they arise.

The Army's force projection precept recognizes that organizations and methods must operate within austere environments. Austerity is certainly not an favorable attribute within the information world. The means and manners of information propagation grow and expand each day, as do attenuate requirements. Austerity may serve the principle of economy of force, but it limits the possibilities for IO engagement, monitoring, and protection.

Information Superiority cannot use Land Dominance as an analogorical design concept. Land Dominance relies upon the use, or threatened use, of destructive force to achieve its purpose. To assume that there exists a parallel within the information world which can be subjected to control and domination is mistaken. The IO environment is so suffusive and permeating that to attack or control a single element of an enemy system will inevitably and unpredictably effect ancillary systems as well.

Swift and decisive action cannot be the hope of IO. Rapidity requires that goals and objectives can be clearly understood and ultimately attainable. Information appliances may be subject to measures of control or destruction, but long-term effects cannot be definitively predicted. Control of targeted systems may indeed result in short-term gains. However, sparing total physical

destruction, the inherent flexibility of information networks reduces these temporary advantages over the course of time.

Standing procedures and lasting practices serve little value as to IO forces. While clearly defined operating methods simplify organization and training, they serve as avenues for hostile attack as well. As IO goals must be clear and unambiguous, the ways and means must remain flexible and adaptive.

The Army has taken great strides toward countering conventional, physical threats in the 21st Century, but it "remains intellectually and structurally mired in the Cold War planning environment of preparation for ... conventional war against like adversaries."[85] The doctrine which evolves from a revised FM 100-5 will undoubtedly support limited, selective employment of destructive force against well-identified threats to national security. However, to apply the presumed reality, design, and language of tomorrow's Army to the development of Information Operations will limit the potential of IO employment and is certain to relinquish information control to secondary prominence once again.

Section 6- Air Force Doctrine and "Air Superiority"

*"The advent of air power, which can go straight to the **vital centers** and either neutralize or destroy them, has put a completely new complexion on the old system of making war. It is now realized that the hostile main army in the field is a false objective, and the real objectives are the vital centers."*

BG William "Billy" Mitchell, 1930[86]

"War can be won from the air."

COL John A. Warden[87]

Like the Army, the Air Force has set about to revise and update its doctrine. While many references are available, a model for Air Force doctrine can be developed from two key resources. Primary is the central doctrinal document, AFDD 1, Air Force Basic Doctrine. The second exists not within a single publication, but rather is drawn from the compendium of works which express the service's 'systems approach' to warfare.

AFDD 1 lists the core competencies upon which all doctrinal percepts are based. Of these, four most accurately describe the 'cultural perspective' of the Air Force. These capabilities are: Air Supremacy; Precision Engagement; Global Attack; and, Rapid Global Mobility.[88] The *systems approach* to warfare is based upon the premise that adversarial forces are defeated when the systems upon which they depend are rendered inoperable.

Air Force doctrine states that Air Supremacy is requisite and the preliminary step to all military operations. Through this 'Command of the Air', friendly forces are provided freedom to conduct all other forms of military maneuver.[89] Air power theorists maintain this as the decisive component of modern warfare. They offer that "no state has lost a war while it maintained air superiority, and attainment of air superiority has been a prelude to military

victory."[90] It is deemed so vital that some infer that air superiority should be considered as an end to itself.[91]

Precision Engagement is likened to the abilities of a skillful surgeon. The accuracy of modern weapons is seen as "providing the scalpel"[92] for 'surgical strikes'. Ever-increasing "precision will come to suggest not only that a weapon strike exactly where it is aimed, but also that the weapons be precise in destroying or affecting only what is supposed to be affected."[93] It raises the expectation that "air strikes [can] be almost entirely confined to military targets."[94] In describing the aftermath of recent operations in Kosovo, CJCS GEN Shelton reported that the unerring capability displayed during Operation "Allied Force represented the most precise bombing in history."[95] John Tirpak submits that "precision guided munitions made Allied Force possible."[96]

AFDD 1 describes the Air Force as "a global strategic power that can protect national interests and achieve national objectives by rapidly projecting potent air power anywhere on earth."[97] Global Attack and Rapid Global Mobility reflect the service's response to force drawdowns and reductions in overseas presence. During recent reorganization initiatives, the majority of strategically positioned forces were replaced by continentally-based, tailorable Air Expeditionary Forces.[98] As a CONUS force, it must possess the ability to "move within hours to any point on the globe without reliance on en route bases."[99]

The systems approach to warfare, now prominent throughout Air Force doctrine, was codified by COL John Warden. This strategy asserts that enemy forces consist of numerous, interdependent, and definable systems. It uses a

five-ring analogy to enounce that effective air strategies must target an adversary's leadership, energy and resources, infrastructure, population, and armed forces.[100]

The enemy must viewed as a complex system whose entire organizational structure and related activities must be attacked.[101] The goal of systemic attack is to selectively assault or threaten those strategic targets that most directly support war making-ability. Selective and simultaneous application of force against key systems is referred to as 'Parallel Warfare'.[102] The net result is to "impose strategic or operational paralysis"[103] - the inability of an enemy to continue a particular course of action. AFDD 1 describes Warden's concept as a new view of conflict realized through the ability to produce a rapid and decisive halt to hostile operations.[104] It continues by proposing that "history... has proven that air power does now have the potential to be the *dominant* and, at times, *decisive* element"[105] in war.

The Air Force has traditionally maintained a service-centric approach to controlling its forces. Employment is based upon the principles of firepower, mobility, and flexibility. While its many subelements serve functions as diverse as airlift support, search and rescue, and strategic surveillance, it is the combatant components around which the force is organized. In 1938, Army Air Corps GEN Frank Andrews stated: "The airplane is the only weapon which can engage with equal facility, land, sea, and other forces..."[106] While Air Force doctrine acknowledges the Principles of War as presented by Joint Doctrine, it maintains that air power "is intrinsically different from either land or sea power,

and its employment must be guided by axioms different than those surface forces."[107]

With this premise, it is little wonder the Air Force perceives its sole reason for being as to rapidly provide long-range, strategic strike capability, all the while resisting efforts to divert assets from these missions. Recent operations in the Middle East and Balkans have reinforced this position. Proponents suggest that "in the United States, especially, elected officials continually call on airpower to project a US or US-led coalition force decisively from above in any situation where action is demanded but where the commitment of ground troops could lead to casualties or long-term involvement."[108] Earl Tifford continues this thought, stating that US "air power and air power alone was the instrument of choice for demonstrating NATO resolve in opposition to Yugoslav actions in Kosovo".[109]

A model of Air Force doctrine would be as follows: It consists of a continentally-based force of rapid, global mobility. It interacts with its operational environment only during crisis, and then, in a temporary and transitory manner. It is reliant upon the ability to apply precise, destructive force against a clearly defined enemy infrastructure, thereby eliminating collateral effects. Simultaneous incapacitation of enemy processes generates 'systemic shock', rapidly and decisively ending conflict. The model presumes an environment in which forces can operate with impunity. It is insular, requiring minimal assistance from supporting forces. This is the model ideal the Air Forces seeks to achieve. Can Information Operations base its doctrine on such an ideal?

An insular IO model will suffer many of the same challenges as the isolated Army. Lone existence effectively removes information operations from the broader environment to which it belongs. This detachment, combined with the rapid 'mobility' of information, interprets a reactive doctrine driven by events rather than by objectives.

As previously demonstrated, Information Superiority is a questionable concept. Even were it possible, achieving this end would undoubtedly require the dedication of the entire military information system. It presumes that once achieved, information assurance can be maintained and affords information impunity. It must discount an adversary's ability to circumvent information security measures. Finally, to assume that information superiority is necessary to ensure victory or avoid defeat is pure conjecture.

The core competencies of air power rely heavily upon exacting engagement. Precise operations are not possible within the IO realm. The interconnectedness of information infrastructures preclude the likelihood that selective engagement will only affect targeted systems.

The 'five-ring' systems theory appears to provide "an easy way to categorize information and understand the relative importance of any particular bit".[110] This assumes that enemy forces will present a recognizable form which can be identified. The constant development and evolution of vast arrays of information technologies renders this unlikely. To presume that from amongst the myriad of systems a critical center of gravity can be discovered is unrealistic. Similarly, to execute an information operation across an entire array of systems,

aiming toward 'strategic information shock' again discounts an enemy's ability to adapt and respond in kind.

Reactively targeting enemy information systems is, in essence, a method of structuring one's own system. Modifying information architectures to match or counter the capabilities of a foe is to engineer predictability and susceptibility within oneself. Predictability is to broadcast strategy. Continual adaptation provides increased security, not increased vulnerability.

Current Air Force doctrine relies heavily upon the concept of systemic shock. It assumes that a properly executed Single Integrated Operational Plan (SIOP) of parallel warfare cannot be defeated. The truth of this hypothesis is unknown and theoretical at best.[111] In his essay, Parallel Warfare and Hyperwar, COL Richard Szafranski provides techniques by which such attacks can be defeated. These methods apply equally to information operations.

When subjected to information control, an enemy will transform his mode of operation. Important information will be disguised, diversified, and dispersed. The threat of information assault will result in preemptive attacks to minimize the effects of both.[112] While these actions may not result in a strategic information reversal, they will certainly mitigate the impact of friendly actions.

The concept of selective concentration of force does not translate to IO. Concentration figuratively puts all the IO 'eggs in one basket' - a desirable target for any adversary. It implies a well-defined informational goal by which tactical action is clearly linked to strategic and political endstates. This linkage rarely exists in peacetime, much less in times of crisis.

Rapid, decisive information operations reside within the realm of theory and speculation. Information campaigns commence well before conventional war begins. They comprise long-standing issues, requiring graduated solutions. So while the theory of parallel information warfare may appear appropriate, it is as equally difficult to define as to execute. A structured approach might theoretically aid in apportioning IO forces and efforts, but such a mechanistic template has little practically in the real world.

Section 7- Naval Doctrine and "Command of the Sea"

"A man-of-war is the best ambassador."

Oliver Cromwell, 1650[113]

"The seas are no longer a self-contained battlefield. Today they are a medium from which warfare is conducted. The oceans of the world are the base of operations from which navies project power unto land areas and targets. The mission of protecting sealanes continues in being, but the Navy's central missions have become to maximize its ability to project power from the sea over the land and to prevent the enemy from doing the same."

Timothy Shea, Project Poseidon, 1961[114]

The history of US naval doctrinal development is distinctive among the services. Prior to the early 1990s, most naval thought was conferred as 'maritime strategy'. Unlike the Army and Air Force, which traditionally establish and promote centralized, enduring principles of organization, employment, and control, little was written of naval doctrine. Despite the existence of a strategy, daily operations were governed moreover from precepts developed throughout time from experience in warfighting and lessons of history.[115] Before the formation of Naval Doctrine Command (NDC)[116] and publication of Naval Doctrinal Publication 1 (NDP 1), Naval Warfare, a codified and comprehensive doctrine did not exist. In fact, it could be contended that the US Navy had no doctrine at all.

In 1992, the Department of the Navy published the 'White Paper' "... From the Sea".[117] This watershed document recognized the need to shift from a Cold War strategy to a doctrine of forward presence and force projection.[118] It summoned a departure from principles of open sea (blue water) global control to littoral (near-land) operations by which to influence events on land.

That same year, the Navy formed its first centralized command

responsible for the formulation of service-wide doctrinal publications.[119] The changing political situation, fiscal and personnel reductions, and uncertain forecasts of regional involvement summoned a reevaluation of naval policy. This produced the most important change in US naval strategic thought this century. And so, the Navy began its first significant and systematic attempt to capture informal maritime precepts within standardized doctrine.[120]

"... From the Sea", and its 1994 revision "Forward... From the Sea", advance new strategic concepts[121] which are summarily translated within NDP 1.[122] These landmark documents express the changing role of the US Navy as an adaptation to emerging threats.[123] They identify the five (5) key roles of US naval forces: Strategic Deterrence; Forward Naval Presence; Sea Control and Maritime Supremacy; Power Projection from the Sea to Land; and, Strategic Sealift.[124] It is upon these, a model can be developed for naval doctrine.

The peacetime organization of the US Navy is based upon two formations; the Aircraft Carrier Battle Groups and the Amphibious Ready Groups.[125] These formal, generic structures are the primary means to appropriate funds and apportion ships among the hemispheres. Conversely, they do not dictate the organization of these forces on a day-to-day basis.

The Navy is operationally employed as Task Forces (and Task Groups). Task forces represent Battle and Ready Groups inured by political, economic, and military influences. When navy ships combine as task forces, they effectively "translate current policy, available resources, current strategy and campaign concepts, threats, lessons learned, technologies, strategic culture, into

tactics, techniques, and procedures that are used by fleet forces to carry out individual unit tasks."[126]

These formations are unique among the services. Whether at peace or war, only the Navy raises and maintains proportionate complements of sea, land, and air power within its primary organization. Regardless of destination, Navy task forces operate with intrinsic offensive, defensive, and security capabilities. Designs ensure independence of operation from the logistical standpoint as well. With inherent support structures, they can rapidly and economically shift priority and location without the need to quarter the force. These qualities produce proficiency in operational tailoring and an unmatched operational endurance.

Operational endurance sustains the key tenets of strategic *deterrence* and *forward presence*; which most certainly and intrinsically shape the Navy's 'cultural perspective'. Notwithstanding combatant requirements, the doctrine recognizes the "most important role ... in situations short of war is to be *engaged* in forward areas, with the objectives of *preventing* conflict and *controlling crisis*".[127] The strategic importance of forward-positioning is reinforced on nearly every page of NDP 1.

Proximity allows naval forces to attain an understanding of their many and dissimilar operational areas. This knowledge is the practical foundation for daily operations and serves as the basis for crisis response. Continually required to do so, task forces are better able to match capability to environment than other services.

Presence is key to implementing strategies of engagement. By habitually operating in friendly, neutral, and potentially-hostile environments, the Navy demonstrates US commitment to allies, underwrites regional stability, promotes cooperation, and maintains a closeness to regional concerns. This translates critical requirements into skills practiced daily in actual theaters of operation, rather than the sterile, non-threatening terrain of CONUS training posts.[128] More importantly, they are active participants, shaping the very constitution of their regions. The force maintains an immediate readiness for combat, all the while engaged to preserve peace.[129]

The organizational and operational foundations of naval task forces are based on local requirements and formulated by regional Commanders in Chief (CINCs). Theater Engagement Plans (TEPs) serve to guide the structure of these forces and prepare them to meet a wide variety of missions; from observation to maritime control, humanitarian relief to combatant operations.

Inherently organized for *deterrence*, the Navy represents the only service which dedicates the majority of their doctrinal prescription to the execution of such missions. The 'just over the horizon' staying power of the Navy serves as the acme of persuasion.[130] It displays national intent and capability in areas deemed vital[131] and demonstrates that US intervention is available and credible. In this manner, the Navy performs virtually the same operational role and tactical tasks in both war and peace.

NDP 1 highlights the distinctiveness of the sea environment. The recent variations in operational focus alters the service's outlook for controlling the

maritime domain, that is - *'Command of the Sea'*. During the Cold War, Command of the Sea was focused to the global threat presented by the USSR. Today the emphasis is regional and less distinct. Navy doctrine updates Command of the Sea now to entail: protecting salines of communications; establishing areas of operations from which to project power; denying enemy commercial and military use of sealanes; and, protecting military infrastructure.[132]

Together they summarize the essence of 'freedom of navigation'. Navy doctrine is atypical, prescribing habitual sojournment and mobility from 'sea bases', freed from political encumbrances that inhibit employment of land and air forces.[133] Inherent portability allows the Navy to reside and move within limits to strike an enemy force, while maintaining the ability to rapidly relocate beyond hostile reach and decrease vulnerability.[134] NDP 1 recognizes that while regional control of the sea may be a prerequisite to some military operations, it has distinct spacial and temporal limitations and can only be applied to specific regions for limited periods of time.[135]

The Navy is the only service to habitually arrange routine operations in order to achieve intents coincidently governed by external political, diplomatic, economic, and geographic considerations. While absolute dominion might be admissible from one perspective, naval forces must concede neutrality within the expanse of the sea environment, and actions ought not encumber the maritime freedom of nonpartisan nations. Theater Engagement Plans seek equally to monitor and curtail movement of others as to maintain freedom for movement of

friendly and allied forces.[136] Absolutely denial to navigational rights of hostile actors - that which precludes rather than temporarily coerce - requires the eventual destruction of that force. Comprehensive and restrictive Command of the Sea is therefore regarded as a final recourse.[137]

The Navy describes doctrine as the Art of the Admiral.[138] It is unusual in that organization, employment, and control begin with the premise that naval forces are active participants and daily instruments of foreign policy.[139] They promote democracy, enhance national security, and bolster the economic prosperity of the US and her allies. Each of these long standing goals are fraught with innate complications which cannot be resolved completely and forever.[140] They require persistent, sustained, and recurring enterprise for which the Navy is exceptionally suited.

Navy doctrine recognizes that sea power may be decisive only in deterrence. Alone, however, it is not the determining element when crisis turns to war.[141] Unlike its sister services, which derive their deterrent advantage through coercive projection of force - the Navy achieves this through overt visibility and proximity. As such, presence is the routine manner of operation and far less provocative than the employment of Army or Air Forces. The Navy possesses the ability to monitor passively, remain on station for extended periods of time, and respond rapidly to crisis. This operational agility likewise allows naval forces to promptly withdraw as situations warrant.[142]

A comparison of the Navy's doctrinal model to that of the Army and Air Force reveals a distinctive approach to warfighting. The 'From the Sea' culture is

particular among the services. Sharing the characteristics of readiness, flexibility, and mobility, the Army and Air Force which observe expeditionary doctrine, while the Navy is expeditionary by its very mode of operation and organization.

The model of naval doctrine is remarkably similar to the revised IO model developed in Section 4. Organizational precepts are based upon inherent capabilities, repackaged to address regional concerns. Supporting both offensive and defensive competencies, it is primarily a doctrine of deterrence. Naval forces respond to emerging threats and vulnerabilities, all the while shaping environments and preventing crises when and where possible.

The information environment conforms to many of the characteristics recognized within the naval domain. Boundaries are ill-defined and encompass friendly, neutral, and hostile interests and vulnerabilities. Active and continual participation mitigates the need for extensive reallocation of resources during crisis and war; ensuring timely response while preserving economy of force. Core competencies are practiced on a daily basis. This not only serves to cultivate regional expertise, but demonstrates national resolve to both allies and foes.

Current principles which describe Command of the Sea parallel the requirements of information control and information superiority. Neither force can operate in a vacuum. Each recognizes that much of the operational environment is neutral and must be governed by enduring notions of freedom of communication - whether navigational or informational.

IO doctrine is likewise a science and an art. The science faces the appliances of IO just as the art addresses nations, organizations, and individuals. It is the art which moreover mandates continual presence, engagement, shaping, and cooperation.

It is reasonable at this junction to survey why naval doctrine happens to so closely resemble the requirements put forth within the revised IO model - making Command of the Sea and Information Superiority profoundly analogous. The answer is founded in a fundamental requirement for higher law; a measure of authority beyond that which is contained in either service or Joint doctrines. A preeminent authority, currently absent from Information Operations doctrine, must be realized if the US is to one day *secure Command of the Cyber-Sea*.

Conclusion - Seeking "Command of the Cyber-Sea"

Information allows the US to "secure peacetime national security objectives, deter conflict, protect information and information systems, and shape the information environment".
DoD Directive S-3600.1, Information Operations[143]

"Information Warfare, as a separate technique of waging war, does not exist."
Martin C. Libicki[144]

Naval operations are inextricably bound by volumes of oceangoing legislation. Whether considering 18th century anti-piracy laws, the London and Washington Naval Treaties of the 1920s[145], or the proposed United Nations Law of the Sea[146], the Navy continually observes standing conventions, agreements, and ordinances, as well as, a host of customs, principles, and etiquettes.

Unlike its CONUS-based Army and Air Force counterparts, the Navy never operates beyond the limits of such statutes. While Laws of Warfare and the many Geneva Accords are imposed during conflict, maritime law is part and parcel to all ocean-bound activities - civilian and military. The Navy willingly surrenders certain measures of control, proscribing power and authority, in order to properly foster the policies advanced by acknowledged civilian leadership.

Although these conventions restrict employment options, they serve an indispensable function in stabilizing an otherwise unbounded and uncontrolled environment. Confrontation at sea is mitigated within this system that subordinates armed forces to international civilian control. These protocols serve to enforce the rule of law, maintain national credibility, protect international trade, and ensure state sovereignty. Without these 'Rules of Engagement', maritime chaos would overtake peaceful coexistence resident upon the oceans.

The information age has created new demands on policy makers and war planners alike. Operating in a similarly turbulent environment, international rules of engagement (ROE) must be established for Information Operations. ROE for IO would stipulate global guidelines specifying under what conditions IO and IW could be used to satisfy political and military demands. They would delineate the circumstances and limitations under which nations would initiate and/or continue IW with other nations.[147] Such rules would moderate the risks associated with centralized policy making and decentralized policy execution by authorizing the varying levels of national, strategic, operational, and tactical command to decide when and how to employ information warfare. Finally, these ROE would serve as yet another visible sign of ongoing US engagement.

Enacting and enforcing IO ROE will be complex. It will require domestic and international consensus between political, economic, and military leaders. It must specify the roles, prerogatives, and utility of international instruments such as NATO or the UN. It must accord treaty obligations, commercial interests, and national constituencies for or against certain actions. The roles, missions, and expectations of military organizations must be adequately defined in uni- and multinational, interagency, and interservice terms.

President Clinton has stipulated that the National Critical Infrastructure Protection Plan be in effect by May 2001 - and fully operational by the end of 2003.[148] Without the delineation of international laws and regulations governing Information Operations, this goal is impractical. The US government must initiate ROE legislation. Its role must be a combination of leadership and

cooperation within the world community.[149] Without these, US IO capabilities will be unrecognized as legitimate forms of action in peace and war. Unsanctioned information operations, especially those with indeterminate results, can only serve to damage US and international security. National credibility is the primary assurance protecting US citizens around the world. Such occurrences will effectively erode confidence in the United States as a world leader.

While 'International Informational Law' may never reach the pinnacle of Maritime Law, the framework has some utility. Perhaps if these standards are enacted and promulgated, other maritime principles can be applied. The information environment may one day employ information interdiction operations similar to the flexible deterrent options currently exploited by the Navy. The time may come when 'third-wave' information convoys, blockades, quarantines, and embargos are added to the global lexicon.

Warfare remains about human beings, human aspirations, and human passions. No one should thoughtfully relegate any manner of engagement or warfare to sterile technology or targets that reside within precisely defined systems. Information Operations need rational, enduring, authoritative concepts to for the much needed 'cultural perspective' for Command of the Cyber-Sea.

ENDNOTES

1. Joint Chiefs of Staff, Joint Doctrine For Information Operations, Joint Publication 3-13 (JP 3-13)(Washington, DC: US Government Printing Office, 9 October 1998), I-15.

2. Roger C. Molander, et al. Strategic Information Warfare: A New Face of War, Santa Monica, CA: RAND, 1996, 1.

3. Office of the Chairman, Joint Chiefs of Staff, Information Operations: A Strategy for Peace, The Decisive Edge in War (Washington, DC: US Government Printing Office, March 1999), 4.

4. Alvin and Heidi Toffler, War and Anti-War (Boston: Little, Brown and Company, 1993), Ch. 1.

5. Thomas J. Kardos, "INTEL XXI and the Maneuver Commander - Redefining Execution of Tactical Intelligence Operations." (MMAS Monograph, School of Advanced Military Studies, 2000.), 2.

6. LTC Bill Flynt, "Threat Convergence," Military Review, (Sep-Oct 99), 3.

7. Department of the Army, Information Operations, FM 100-6 (Washington DC: US Government Printing Office, 27 August 1996), I-6/7.

8. Molander, 1.

9. DR Robert Stark, "Future Warfare: Information Superiority Through Info War." (Research Study, Department of Defense and Strategic Studies, Southwestern Missouri University: 1999, from Internet: smsu.edu, accessed: 16 Feb 2000), 7.

10. John Arquilla, et al. In Athena's Camp: Preparing for Conflict in the Information Age, Santa Monica, CA: RAND, 1997, 7.

11. Office of the Secretary of Defense, 1998 Annual Report of the Quadrennial Defense Review (Final Report, Washington, DC: US Government Printing Office, 1998), 4.

12. Joint Chiefs of Staff, DoD Dictionary of Military and Associated Terms, Joint Publication 1-02 (Washington, DC: US Government Printing Office, 1999), 103.

13. DR James J. Tritten, "Naval Perspectives for Military Doctrine Development." (White Paper, Naval Doctrine Command, Norfolk, VA: 1994), 13.

14. Department of the Army, Operations, FM 100-5 (Washington DC: US Government Printing Office, 27 August 1996), I-1.

15. Ibid., and Tritten, 15.

16. Christopher Bellamy, The Evolution of Modern Land Warfare - Theory and Practice (New York: Routledge, 1990), 10-13.

17. The White House, A National Security Strategy for a New Century (Washington, DC: US Government Printing Office, December 1997), 14.

18. Stark, 7.

19. Ibid.

20. Information Operations: A Strategy for Peace, The Decisive Edge in War, 4.

21. FM 100-6, 1-1.

22. LTC Alan T. Evans, "Department of Defense in the Age of Information Operations." (US Army War College, Carlisle Barracks, PA: 13 May 1998), 4.

23. The President's Commission on Critical Infrastructure Protection, Critical Foundations Protecting America's Infrastructures, (Final Report, Washington, DC: October 97), 8.

24. Information Operations: A Strategy for Peace, The Decisive Edge in War, 1.

25. Jeffery Record, "Operation Allied Force: Yet Another Wake-Up Call for the Army?" Parameters (Winter 99-00), 21.

26. JP 3-13, I-13.

27. National Defense Panel, Transforming Defense - National Security in the 21st Century (Final Report, Washington, DC: December 97), 13.

28. FM 100-6, 1-10.

29. Molander, 3.

30. Office of the Chairman, Joint Chiefs of Staff, Joint Vision 2010 (Washington, DC: US Government Printing Office, May 1997), 15-18.

31. FM 100-6, 1-4.

32. LTC Timothy L. Thomas, "Human Network Attacks," Military Review (Sep-Oct 99), 23.

33. Ibid., iv.

34. Ibid., 2.

35. Kardos, 6-7.

36. Joint Vision 2010, 16.

37. Ibid., 1.

38. Information Operations: A Strategy for Peace, The Decisive Edge in War, 5.

39. FM 100-6, iv.

40. Department of the Army, LIWA: Information Operations (IO) k [Draft] (US Army Land Information Warfare Activity, Fort Belvoir, VA: October 1998), 1-1.

41. JP 3-13, vi.

42. Information Operations: A Strategy for Peace, The Decisive Edge in War, 5.

43. Ibid.

44. Ibid.

45. Martin C. Libicki, "What Is Information." (Research Study, Center for Advanced Concepts and Technology, Institute for National Strategic Studies, National Defense University, US Government Printing Office, Washington, DC: August 1995), ix.

46. JP 3-13, vi.

47. Commander Bryan Q. Clemmons and MAJ Gary D. Brown, "Targets in Cyberspace: Cyberwarfare - Ways, Warriors, and WMD," Military Review (Sep-Oct 99) 35.

48. Information Operations: A Strategy for Peace, The Decisive Edge in War, 5.

49. Libicki, x.

50. LIWA, 1-1.

51. Stark, 10.

52. JP 3-13, ix.

53. Ibid.

54. Ibid., I-6.

55. Information Operations: A Strategy for Peace, The Decisive Edge in War, 3.

56. LIWA, 1-3.

57. Information Operations: A Strategy for Peace, The Decisive Edge in War, 4.

58. Ibid., Chapter 1.

59. Libicki, 4.

60. Ibid., ix.

61. JP 3-13, I-13.

62. JP 3-13. I-1.

63. Clemmons, 37.

64. LIWA, 1-11 thru 1-13.

65. Evans, 9.

66. MAJ Vincent D. Bryant, "Changing the Azimuth of Information Operations." (Masters Paper, Naval War College, Newport, 10 February 1998) 17.

67. Tritten, 4.

68. Ibid., 7.

69. LTC Lester W. Grau and Jacob Kipp, "Urban Combat: Confronting The Specter," Military Review (Jul-Aug 1999), 9.

70. William F. Grimsley, "Intelligence Preparation of the Future Operational Battlefield," (MMAS monograph, School of Advanced Military Studies, 1994.), 5.

71. FM 100-5, v.

72. Department of the Army, INTEL XXI: A Concept for Force XXI Intelligence Operations, TRADOC Pamphlet 525-75 (Fort Monroe, VA: TRADOC, 10 January 1996), 2-15.

73. Ibid., 1-1.

74. "Fast Facts", Army Times, 1 May 00, 2.

75. TRADOC Pam 525-75, 2-15.

76. Ibid., 1.

77. LTC Larry D. Bruns, "Threat Theory, A Model for Forecasting the Threat Environment of the Future," (Fort Leavenworth, School of Advanced Military Studies, 21 Apr 1993), 41.

78. A National Security Strategy for a New Century, 1999, 3.

79. Ibid., 19.

80. Tritten, 12.

81. FM 100-6, iv.

82. TRADOC Pamphlet 525-75, 2-5.

83. Ibid.

84. Ibid., 1-2.

85. Record, 19.

86. Headquarters Air Force Doctrine Center, Air Force Basic Doctrine, AFDD 1 (Maxwell AFB, AL: September 1997), 45.

87. COL John A. Warden, III, The Air Campaign: Planning for Combat. (National Defense University Press, Washington, DC: 1988), 39.

88. AFDD 1, 27.

89. Ibid., 29.

90. Warden, The Air Campaign, 13.

91. Ibid., 63.

92. AFDD 1, 30.

93. COL John A. Warden, III, "Air Theory for the Twenty-first Century," Battlefield of

the Future: 21st Century Warfare Issues, Barry R. Schneider and Lawrence E. Grinter, eds. (Air University Press, Maxwell AFB, AL: 1998), 103.

94. John A. Tirpak, "The State of Precision Guided Munitions," Air Force Journal (March 2000), 25.

95. Ibid., 26.

96. Ibid., 25.

97. AFDD 1, Forward.

98. Ibid., 67-68.

99. Warden, "Air Theory...", 103.

100. Barry R. Schneider and Lawrence E. Grinter, "Overview: Future Airpower and Strategy Issues," Battlefield of the Future: 21st Century Warfare Issues. (Air University Press, Maxwell AFB, AL: 1998), 99.

101. Warden, "Air Theory...", 108.

102. COL David A. Deptula, "Firing for Effect: Change in the Nature of Warfare." (Aerospace Education Foundation, Arlington, VA: 1995), 5.

103. Schneider and Grinter, 99.

104. AFDD 1, 42.

105. Ibid., 41-42.

106. Ibid., 11.

107. Ibid., 21.

108. Chris and Janet Morris, and Thomas Baines, "Weapons of Mass Protection: Nonlethality, Information Warfare, and Airpower in the Age of Chaos." (Air University, Maxwell AFB, AL: 1998), 3.

109. Tifford, 27.

110. Warden, "Air Theory...", 108.

111. Tifford, 34.

112. COL Richard Szafranski, "Parallel War and Hyperwar: Is Every Want a Weakness?" Battlefield of the Future: 21st Century Warfare Issues, Barry R. Schneider and Lawrence E. Grinter, eds. (Air University Press, Maxwell AFB, AL: 1998), 139-140.

113. Department of the Navy, Naval Warfare, NDP 1 (Washington DC: US Government Printing Office, 1994), Ch. 1, 4.

114. Ibid., Ch. 1, 5-6.

115. Ibid., Forward, 1.

116. Ibid., 3.

117. Department of the Navy, "... From the Sea," (White Paper, Washington DC: US Government Printing Office, 1992), cover letter.

118. Ibid., 4.

119. Tritten, 3.

120. Ibid., 7.

121. "... From the Sea", cover.

122. Ibid.

123. Naval Warfare, Ch. 1.

124. "... From the Sea", 10.

125. Ibid., 3.

126. Tritten, 7.

127. Ibid., Introduction.

128. Naval Warfare, Ch. 1, 5.

129. "... From the Sea", 10.

130. Naval Warfare, Forward, 2.

131. "... From the Sea", 2.

132. Naval Warfare, Ch. 2, 8.

133. "... From the Sea", 5.

134. Naval Warfare, Ch. 1, 7.

135. Ibid., Ch. 2, 9.

136. Ibid.

137. Herbert Rosinski, The Development of Naval Thought: Essays by Herbert Rosinski. (Naval War College Press, Newport, RI: 1977) 4.

138. Tritten, 15.

139. "... From the Sea", 3.

140. The White House, A National Security Strategy for a New Century (Washington, DC: US Government Printing Office, December 1999), 3.

141. Naval Warfare, Ch. 2, 10.

142. Ibid., Ch. 1, 7.

143. US Department of Defense, Information Operations, DoD Directive S-3600.1 (Washington DC: US Government Printing Office, 9 Dec 1996), paragraph D.1.

144. Libicki, x.

145. Russell F. Weigley, The American Way of War: A History of US Military Strategy and Policy (Indiana University Press, Bloomington: IN, 1973), 243-245.

146. NSS, 12.

147. Department of the Army, Operational Terms and Graphics, FM 101-5-1 (Washington DC: US Government Printing Office, 30 September 1997), I-135.

148. NSS, 17.

149. Molander, 6-7.

BIBLIOGRAPHY

BOOKS

Arquilla, John. In Athena's Camp: Preparing for Conflict in the Information Age. Santa Monica, CA: RAND, 1997.

Bellamy, Christopher. The Evolution of Modern Land Warfare - Theory and Practice. New York: Routledge, 1990.

Molander, Roger C. Strategic Information Warfare: A New Face of War. Santa Monica, CA: RAND, 1996.

Rosinski, Herbert. The Development of Naval Thought: Essays by Herbert Rosinski. Newport, RI: Naval War College Press, 1977.

Schneider, Barry R. and Lawrence E. Grinter, "Overview: Future Airpower and Strategy Issues," Battlefield of the Future: 21st Century Warfare Issues. Maxwell AFB, AL: Air University Press, 1998.

Toffler, Alvin and Heidi. War and Anti-War: Surviving at the Dawn of the 21st Century. Boston: Little, Brown and Company, 1993.

MONOGRAPHS & PAPERS

Bryant, Vincent D., MAJ. "Changing the Azimuth of Information Operations." Master Paper, Newport, RI: Naval War College, 10 February 1998.

Deptula, David A., COL. "Firing for effect: Change in the Nature of Warfare." Booklet, Arlington, VA: Aerospace Education Foundation, 1995.

Evans, Alan T., COL. "Department of Defense in the Age of Information Operations." Research Paper, Carlisle Barracks, PA: US Army War College, 1998.

Grimsley, William F., MAJ. "Intelligence Preparation of the Future Operational Battlefield." MMAS monograph, Fort Leavenworth, KS: School of Advanced Military Studies, 1994.

Kardos, Thomas J., MAJ. "INTEL XXI and the Maneuver Commander - Redefining Execution of Tactical Intelligence Operations." MMAS Monograph, Fort Leavenworth, KS: School of Advanced Military Studies, 2000.

Libicki, Martin C. "What Is Information Warfare?" Research Study, US

Government Printing Office, Washington, DC: National Defense University, Center for Advanced Concepts and Technology, Institute for National Strategic Studies, August, 1995.

Morris, Chris and Janet, and Thomas Baines. "Weapons of Mass Protection: Nonlethality, Information Warfare, and Air Power in the Age of Chaos." Research Study, Maxwell AFB, AL: Air University, 2000.

Stark, Robert, Dr. "Future Warfare: Information Superiority Through Info War." Research Study, from Internet: smsu.edu: Southwestern Missouri University, accessed: 16 February 2000.
Leavenworth, KS: School of Advanced Military Studies, 2000.

Tritten, James R., Dr. "Naval Perspectives for Military Doctrine Development." White Paper, Norfolk, VA: Naval Doctrine Command, 1994.

Warden, John A., COL. "Air Theory for the Twenty-first Century," Battlefield of the Future: 21st Century Warfare Issues. Barry R. Schneider and Lawrence Grinter, ed., Maxwell, AFB, AL: Air University Press, 1998.

Szafranski, Richard, COL. "Parallel War and Hyperwar: Is Every Want a Weakness?" Battlefield of the Future: 21st Century Warfare Issues. Barry R. Schneider and Lawrence Grinter, ed., Maxwell, AFB, AL: Air University Press, 1998.

ARTICLES

Bruns, Larry D. "Threat Theory, A Model for Forecasting the Threat Environment of the Future." Fort Leavenworth, KS: School of Advanced Military Studies, 21 Apr 1993.

Clemmons, Byran Q., and MAJ Gary D. Brown. "Targets in Cyberspace: Cyberwarfare - Ways, Warriors, and WMD." Military Review Vol. LXXIX, No. 5 (Sep-Oct 99): 35-45.

Flynt, Bill. "Threat Convergence." Military Review Vol. LXXIX, No. 5 (Sep-Oct 99): 2-11.

Grau, Lester W., and Jacob Kipp. "Urban Combat: Confronting the Specter." Military Review Vol. LXXIX, No. 4 (Jul-Aug 99): 9-17.

Record, Jeffery. "Operation Allied Force: yet Another Wake-up Call for the Army?" Parameters Vol. XXIX, No. 4 (Winter 99-00): 15-23.

Thomas, Timothy L. "Human Network Attacks." Military Review Vol. LXXIX, No. 5 (Sep-Oct 99): 23-33.

Tirpak, John A. "The State of Precision Guided Munitions." Air Force Journal Vol. 83, No. 3 (Mar 2000): 23-29.

Tifford, Earl H. "Operation Allied Force and the Role of Air Power" Parameters Vol. XXIX, No. 4 (Winter 99-00): 24-28.

GOVERNMENT DOCUMENTS

Department of the Army. Information Operations, FM 100-6. Washington, DC: US Government Printing Office, 27 August 1996.

Department of the Army. Operational Terms and Graphics, FM 101-5-1. Washington, DC: US Government Printing Office, 30 September 1997.

Department of the Army. LIWA: Information Operations (IO) Handbook, Draft, Fort Belvoir, VA: US Army Land Information Warfare Activity, October, 1998.

Department of the Army. Force XXI Operations, TRADOC Pamphlet 525-5. Fort Monroe, VA: TRADOC, 1 August 1994.

Department of Defense. Information Operations. DoD Directive S-3600.1, Washington, DC: US Government Printing Office, 9 December 1996.

Department of the Navy. "White Paper, ... From the Sea." Washington, DC: US Government Printing Office, 1992.

Department of the Navy. Naval Warfare, NDP 1. Washington, DC: US Government Printing Office, 1994.

Headquarters, Air Force Doctrine Center. Air Force Basic Doctrine. AFDD 1. Maxwell AFB, AL: September 1997.

National Defense Panel. Transforming Defense - National Security in the 21st Century. Final Report, Washington, DC: December 1997.

Office of the Chairman, Joint Chiefs of Staff. DoD Dictionary of Military and Associated Terms. Washington, DC: US Government Printing Office 1999.

Office of the Chairman, Joint Chiefs of Staff. Information Operations A Strategy for Peace, The Decisive Edhe in War. Washington, DC: US Government Printing

Office, March 1999.
Office of the Chairman, Joint Chiefs of Staff. Joint Vision 2010. Washington, DC: US Government Printing Office, 1998.

Office of the Secretary of Defense. 1998 Annual Report of thhe Quadrennial Defens Review. Final Report, Washington, DC: US Government Printing Office, 1998.

The President's Commission on Critical Information Infrastruture Protection. Critical Foundations Protecting Amercia's Infrastructures. Final Report, Washington, DC: October, 1997.

Warden, John A., COL. The Air Campaign: Planning For Combat. Washington, DC: National University Press, 1988.

The White House. A National Security Strategy for a New Century. Washington, DC: December, 1997.

The White House. A National Security Strategy for a New Century. Washington, DC: December, 1999.